AMENDMENTS TO THE CLAIMS

Please amend claims 1 and 9 as indicated below.

Pursuant to 37 C.F.R. § 1.121 the following listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims:

Claim 1 (Currently Amended): A method for providing a time stamp by using a tamper-proof time signal via a telecommunications network comprising the steps of:

receiving, at a central system, a request from a network user for a time signal;

encrypting said time signal by the central system with at least one key;

transmitting the encrypted time signal to the network user via the telecommunications network;

providing the network user with the same at least one key; and

synchronously generating~~, at the central system and the network user,~~ the at least one key by a respective clock system of the central system and of the network user uniquely assigned to the network user ~~the at least one key~~.

Claim 2 (Currently Amended): The method as recited in claim 1, wherein the synchronously generating is performed so as to change the at least one key ~~changes~~ synchronously after predetermined time intervals.

Claim 3 (Currently Amended): The method as recited in claim 1, further comprising the steps of:

providing the network user and the central system each with ~~at least one~~ the respective clock system thereof;

respectively assigning the ~~at least one~~ respective clock system ~~at~~ of the network user to the ~~at least one~~ respective clock system ~~at~~ of the central system so that the respectively assigned ~~at least one~~ respective clock ~~system~~ systems operate synchronously to generate the at least one key.

Claim 4 (Currently Amended): The method as recited in claim 1, further comprising the steps of:

receiving a time signal request, at the central system, from the network user; and

determining, by the central system, [[a]] the clock system uniquely assigned to the network user using a transmitted identifier, wherein the transmitted identifier is the network address of the network user~~; and wherein the at least on key is generated by the assigned clock system~~; and

transmitting, by the central system, the encrypted time signal.

Claim 5 (Previously Presented): A method for transmitting data with a tamper-proof time stamp over a telecommunications network from a first network user to a second network user, comprising the steps of:

obtaining a time signal in accordance with a method as recited in claim 1;

transmitting the time signal and the data from the first network user to the second network user one of directly and indirectly via the central system.

Claim 6 (Previously Presented): The method as recited in claim 5, further comprising the steps of:

encrypting, by the first network user, at least one of the data and the time signal during transmission.

Claim 7 (Previously Presented): The method as recited in claim 5, wherein the central system is provided at the second network user.

Claim 8 (Previously Presented): The method as recited in claim 5, further comprising the step of returning, by the central system, an acknowledgement of receipt to the first network user.

Claim 9 (Currently Amended): A system for generating a tamper-proof time stamp in network-based communication systems, the system comprising:

a central system connected to the network-based communication system;

a network user connected to the network-based communication system; and

a respective clock system at the network user and at the central system being uniquely assigned to the network user, wherein each of the respective clock systems is assigned to each other and configured to operate synchronously so as to generate at least one changed key;

wherein the central system is configured to encrypt a time signal using the at least one changed key, and further configured to send the encrypted time signal to the network user; and

wherein the network user is configured to decrypt the encrypted time signal.

Claim 10 (Previously Presented): The system as recited in claim 9, wherein the central system includes a time signal transmitter.

Claim 11 (Currently Amended): The method as recited in claim 1, further including the steps of:

providing ~~the network user and~~ the central system ~~each~~ with at least one respective clock system;

assigning the ~~at least one~~ network user uniquely assigned respective clock system ~~at the network user~~ to the at least one respective clock system at the central system so that the assigned ~~at least one~~ respective clock system operate synchronously to change the at least one key.

Claim 12 (Previously Presented): The method as recited in claim 6, wherein a central system is provided at the second network user.

Claim 13 (Previously Presented): The method as recited in claim 6, wherein the central system is configured to return an acknowledgement of receipt to the first network user.

Claim 14 (Previously Presented): The method as recited in claim 7, wherein the central system is configured to return an acknowledgement of receipt to the first network user.

Claim 15 (Previously Presented): The method as recited in claim 1, further comprising the step of decrypting, by the network user using the at least one key, the transmitted encrypted time signal.

Claim 16 (Previously Presented): The method as recited in claim 1, wherein the central system is a certified central system.

Claim 17 (Previously Presented): The method as recited in claim 1, wherein the time signal is an officially recognized time signal.

Claim 18 (Currently Amended): The method as recited in claim 4, wherein the at least one key is generated by ~~at least one of~~ the uniquely assigned clock system and the transmitted identifier.

Claim 19 (Previously Presented): The method as recited in claim 9, wherein the at least one changed key is synchronously generated at intervals of time.

Claim 20 (Previously Presented): The method as recited in claim 9, wherein the time signal is an officially recognized time signal.